IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTY. DOCKET NO. 040301/0539

In re Patent Application of
Atsushi INOUE et al.
Serial No. Unassigned
Filed: September 4, 1998
For: MOBILE IP COMMUNICATION SCHEME INCORPORATING INDIVIDUAL USER AUTHENTICATION

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. 119, is hereby claimed.

In support of this claim, filed herewith are certified copies of said original foreign applications:

Japanese Patent Applications
No. 9-241163 filed September 5, 1997 and
No. 9-241167 flied September 5, 1997.

Respectfully submitted,

September 4, 1998

for 25144
Richard L. Schwaab
Reg. No. 25,479

FOLEY & LARDNER
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Tel: (202) 672-5300

INOUE et al.
040301/0539

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９７年 ９月 ５日

出願番号
Application Number: 平成 ９年特許願第２４１１６３号

出願人
Applicant (s): 株式会社東芝

１９９８年 ４月１７日

特許庁長官
Commissioner,
Patent Office

荒井寿光

【書類名】　特許願

【整理番号】　A009704681

【提出日】　平成 9年 9月 5日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/00

【発明の名称】　移動計算機管理装置、移動計算機装置、通信システム及び移動計算機登録方法

【請求項の数】　12

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　井上　淳

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　石山　政浩

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　福本　淳

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　津田　悦幸

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　岡本　利夫

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　移動計算機管理装置、移動計算機装置、通信システム及び移動計算機登録方法

【特許請求の範囲】

【請求項１】

ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する移動計算機管理装置であって、

前記移動計算機から発信された現在位置の情報を含む新規の登録メッセージを受信した場合、該移動計算機に対してユーザ認証のための情報の返送を要求するメッセージを送信する手段と、

このメッセージを送信した前記移動計算機から前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、該ユーザ入力に基づく情報を判定して該ユーザの正当性が確認されたならば、該移動計算機の現在位置の登録を許可する手段とを備えたことを特徴とする移動計算機管理装置。

【請求項２】

前記移動計算機から同じ現在位置について再登録を行うための登録メッセージを受信した場合、予め規定されたユーザ認証実行条件が成立するならば、直ぐに再登録をせずに該移動計算機に対して前記ユーザ認証のための情報の返送を要求するメッセージを送信する手段をさらに備えたことを特徴とする請求項１に記載の移動計算機管理装置。

【請求項３】

同一の前記移動計算機について、返送された前記メッセージからは前記ユーザの正当性が確認されなかったことが、予め規定された回数連続した場合には、これ以降は該移動計算機からの登録要求を拒否することを特徴とする請求項１または２に記載の移動計算機管理装置。

【請求項４】

前記移動計算機から前記ユーザ入力に基づく情報として返されたパスワードが

予め登録されたものと一致するか否かによりユーザの正当性を判断することを特徴とする請求項１ないし３のいずれか１項に記載の移動計算機管理装置。

【請求項５】

前記ユーザ認証を要求するメッセージにはチャレンジコードを含め、

前記移動計算機から前記ユーザ入力に基づく情報として返された前記チャレンジコードに基づくワンタイムパスワードを検査することによりユーザの正当性を判断することを特徴とする請求項１ないし３のいずれか１項に記載の移動計算機管理装置。

【請求項６】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、

自装置がホームとするネットワーク外の移動先から、該ホームとするネットワークに設置された、自装置の移動位置情報を管理し、自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを送信する手段と、

この登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求するメッセージを受信した場合、ユーザ認証のための所定のユーザ入力を受け付ける手段と、

このユーザ入力に基づく情報を書き込んだメッセージを前記移動計算機管理装置宛てに返送する手段とを備えたことを特徴とする移動計算機装置。

【請求項７】

返送した前記メッセージに対して前記移動計算機管理装置からユーザの正当性が確認されなかった旨を示すメッセージが送信されてきたことが、予め規定された回数連続した場合には、これ以降の自装置からの登録要求メッセージの送出を抑止することを特徴とする請求項６に記載の移動計算機装置。

【請求項８】

前記ユーザ入力に基づく情報は、自計算機にユーザ入力されたパスワードであることを特徴とする請求項６または７に記載の移動計算機管理装置。

【請求項９】

前記ユーザ入力に基づく情報は、前記ユーザ認証のための情報の返送を要求するメッセージに含まれたチャレンジコードに基づくワンタイムパスワードであることを特徴とする請求項６または７に記載の移動計算機管理装置。

【請求項１０】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機と、この移動計算機のホームとするネットワークに設置され、該移動計算機の移動位置情報を管理し、該移動計算機宛のデータパケットを該移動計算機の現在位置に転送する移動計算機管理装置とを備えた通信システムにおける移動計算機登録方法であって、

前記移動計算機は、自装置がホームとするネットワーク外の移動先で接続された場合、該ホームとするネットワークに設置された前記移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを発信し、

前記移動計算機管理装置は、自装置の管理対象とする前記移動計算機から発信された現在位置の情報を含む新規の登録メッセージを受信した場合、該移動計算機に対してユーザ認証のための情報の返送を要求するメッセージを返信し、

前記移動計算機は、前記移動計算機管理装置から返信された前記ユーザ認証のための情報の返送を要求するメッセージを受信した場合、ユーザ認証のための所定のユーザ入力を受け付け、このユーザ入力に基づく情報を書き込んだメッセージを前記移動計算機管理装置宛てに返送し、

前記移動計算機管理装置は、前記移動計算機から前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、該ユーザ入力に基づく情報を判定して該ユーザの正当性が確認されたならば、該移動計算機の現在位置の登録を行うことを特徴とする移動計算機登録方法。

【請求項１１】

ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する移動計算機管理装置における移動計算機登録方法であって、

前記移動計算機から発信された現在位置の情報を含む新規の登録メッセージを

受信した場合、該移動計算機に対してユーザ認証のための情報の返送を要求するメッセージを送信し、

このメッセージを送信した前記移動計算機から前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、該ユーザ入力に基づく情報を判定して該ユーザの正当性が確認されたならば、該移動計算機の現在位置の登録を許可することを特徴とする移動計算機登録方法。

【請求項１２】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置における移動計算機登録方法であって、

自装置がホームとするネットワーク外の移動先から、該ホームとするネットワークに設置された、自装置の移動位置情報を管理し、自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを送信し、

この登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求するメッセージを受信した場合、ユーザ認証のための所定のユーザ入力を受け付け、

このユーザ入力に基づく情報を書き込んだメッセージを前記移動計算機管理装置宛てに返送することを特徴とする移動計算機登録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、相互接続している複数のネットワーク間で相互にデータを交換し必要なサービスを提供する複数の計算機により構成されるシステムにおける、ネットワーク間を移動して通信を行うことが可能な移動計算機装置、移動計算機の移動位置情報を管理し移動計算機宛のパケットを移動計算機の現在位置に転送する移動計算機管理装置、通信システム及び移動計算機登録方法に関する。

【０００２】

【従来の技術】

計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、一組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【０００３】

また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上を管理し、正しく通信内容を到達させるための方式が必要である。

【０００４】

一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛のＩＰパケットを移動計算機の現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図１では、元々ホームネットワーク１ａに属していた移動計算機２が、他のネットワーク１ｂに移動し、ネットワーク１ｃ内の他の計算機（ＣＨ）３との間で通信を行う場合に、移動計算機

2に対しホームエージェント（ＨＡ）５が上記の役割を行う。この方式は、インターネットの標準化団体であるＩＥＴＦのｍｏｂｉｌｅ－ＩＰワーキンググループで標準化が進められている移動ＩＰと呼ばれる方式である（文献：ＲＦＣ２００２，　ＩＰ　ｍｏｂｉｌｉｔｙ　ｓｕｐｐｏｒｔ　（Ｃ．Ｐｅｒｋｉｎｓ））。

【０００５】

ところで、移動ＩＰ方式では、移動計算機が新規の移動先に移った場合、現在位置の登録メッセージをホームエージェントに送ることが必要である。移動計算機への成り済ましなどの攻撃を回避するため、位置登録メッセージには移動計算機とホームエージェント間で予め交換したセキュリティ情報に従って認証コードが付加される。正しい認証コードが付加された登録メッセージでないと、移動計算機に位置登録は行われない。

【０００６】

しかしながら、移動ＩＰで規定されているセキュリティ対策はあくまでホスト（移動計算機）単位のセキュリティであり、その移動計算機を使用しているユーザの実体を認証するものではない。すなわち、例えば移動計算機にホスト間の認証のためのセキュリティ情報が保持されたまま、不正なユーザにホスト自体が盗まれると、不正なユーザが正規ユーザに成り済まして、ホームネットワークの情報を取り出すことができ非常に危険である。

【０００７】

また、ホストを盗まれなくても、正規ユーザが登録処理までを行った移動計算機を一時的に借用するだけで、ホームネットワーク上の機密情報を取り出されてしまうことも考えられる。

【０００８】

すなわち、従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱いといえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【０００９】

【発明が解決しようとする課題】

従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱いといえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【００１０】

本発明は、上記事情を考慮してなされたもので、移動計算機が移動先ネットワークに接続し、現在位置の登録メッセージをホームエージェントに送信する際に、移動計算機を操作しているユーザを認証することのできる移動計算機管理装置、移動計算機装置、通信システム及び移動計算機登録方法を提供することを目的とする。

【００１１】

また、本発明は、一旦移動計算機が現在位置の登録メッセージをホームエージェントに送信した後も、定期的にユーザ認証を行い、セッション確立後に不正ユーザが移動計算機を使用するケースにも対応できる移動計算機管理装置、移動計算機装置、通信システム及び移動計算機登録方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】

本発明（請求項１）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する移動計算機管理装置（ホームエージェント）であって、前記移動計算機から発信された現在位置の情報を含む新規の登録メッセージを受信した場合、該移動計算機に対してユーザ認証のための情報の返送を要求するメッセージを送信する手段と、このメッセージを送信した前記移動計算機から前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、該ユーザ入力に基づく情報を判定して該ユーザの正当性が確認されたならば、該移動計算機の現在位置の登録を許可する手段とを備えたことを特徴とする。

【００１３】

好ましくは、前記移動計算機から同じ現在位置について再登録を行うための登録メッセージを受信した場合、予め規定されたユーザ認証実行条件が成立するならば、直ぐに再登録をせずに該移動計算機に対して前記ユーザ認証のための情報の返送を要求するメッセージを送信する手段をさらに備えるようにしてもよい。

【００１４】

予め規定されたユーザ認証実行条件としては、例えば、前回にユーザ認証を行ってから予め規定された時間が経過していること、あるいは前回にユーザ認証を行うこととなった再登録を行うための登録メッセージの受信から今回の受信が予め規定された回数に当たること、などが考えられる。

【００１５】

なお、再登録を行うための登録メッセージを受信する毎に毎回、ユーザ認証を行うようにしてもよい。

好ましくは、同一の前記移動計算機について、返送された前記メッセージからは前記ユーザの正当性が確認されなかったことが、予め規定された回数連続した場合には、これ以降は該移動計算機からの登録要求を拒否するようにしてもよい。

【００１６】

好ましくは、前記移動計算機から前記ユーザ入力に基づく情報として返されたパスワードが予め登録されたものと一致するか否かによりユーザの正当性を判断するようにしてもよい。

【００１７】

好ましくは、前記ユーザ認証を要求するメッセージにはチャレンジコードを含め、前記移動計算機から前記ユーザ入力に基づく情報として返された前記チャレンジコードに基づくワンタイムパスワードを検査することによりユーザの正当性を判断するようにしてもよい。

【００１８】

本発明（請求項６）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、自装置がホームとするネットワーク外の移動先から、該ホームとするネットワークに設置された、自装置の移動位置情

報を管理し、自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置（ホームエージェント）宛に、現在位置の情報を含む登録メッセージを送信する手段と、この登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求するメッセージを受信した場合、ユーザ認証のための所定のユーザ入力を受け付ける手段と、このユーザ入力に基づく情報を書き込んだメッセージを前記移動計算機管理装置宛てに返送する手段とを備えたことを特徴とする。

【００１９】

好ましくは、返送した前記メッセージに対して前記移動計算機管理装置からユーザの正当性が確認されなかった旨を示すメッセージが送信されてきたことが、予め規定された回数連続した場合には、これ以降の自装置からの登録要求メッセージの送出を抑止するようにしてもよい。

【００２０】

好ましくは、前記ユーザ入力に基づく情報は、自計算機にユーザ入力されたパスワードであってもよい。

好ましくは、前記ユーザ入力に基づく情報は、前記ユーザ認証のための情報の返送を要求するメッセージに含まれたチャレンジコードに基づくワンタイムパスワードであってもよい。

【００２１】

本発明（請求項１０）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機と、この移動計算機のホームとするネットワークに設置され、該移動計算機の移動位置情報を管理し、該移動計算機宛のデータパケットを該移動計算機の現在位置に転送する移動計算機管理装置（ホームエージェント）とを備えた通信システムにおける移動計算機登録方法であって、前記移動計算機は、自装置がホームとするネットワーク外の移動先で接続された場合、該ホームとするネットワークに設置された前記移動計算機管理装置宛に、現在位置の情報を含む登録メッセージを発信し、前記移動計算機管理装置は、自装置の管理対象とする前記移動計算機から発信された現在位置の情報を含む新規の登録メッセージを受信した場合、該移動計算機に対してユーザ認証のための情報の返送

を要求するメッセージを返信し、前記移動計算機は、前記移動計算機管理装置から返信された前記ユーザ認証のための情報の返送を要求するメッセージを受信した場合、ユーザ認証のための所定のユーザ入力を受け付け、このユーザ入力に基づく情報を書き込んだメッセージを前記移動計算機管理装置宛てに返送し、前記移動計算機管理装置は、前記移動計算機から前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、該ユーザ入力に基づく情報を判定して該ユーザの正当性が確認されたならば、該移動計算機の現在位置の登録を行うことを特徴とする。

【００２２】

本発明（請求項１１）は、ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し、該移動計算機宛のパケットを該移動計算機の現在位置に転送する移動計算機管理装置（ホームエージェント）における移動計算機登録方法であって、前記移動計算機から発信された現在位置の情報を含む新規の登録メッセージを受信した場合、該移動計算機に対してユーザ認証のための情報の返送を要求するメッセージを送信し、このメッセージを送信した前記移動計算機から前記ユーザ認証のための情報として該移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、該ユーザ入力に基づく情報を判定して該ユーザの正当性が確認されたならば、該移動計算機の現在位置の登録を許可することを特徴とする。

【００２３】

本発明（請求項１２）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置における移動計算機登録方法であって、自装置がホームとするネットワーク外の移動先から、該ホームとするネットワークに設置された、自装置の移動位置情報を管理し、自装置宛のパケットを自装置の現在位置に転送する移動計算機管理装置（ホームエージェント）宛に、現在位置の情報を含む登録メッセージを送信し、この登録メッセージを受信した前記移動計算機管理装置から返信された、ユーザ認証のための情報の返送を要求するメッセージを受信した場合、ユーザ認証のための所定のユーザ入力を受け付け、このユーザ入力に基づく情報を書き込んだメッセージを前記移動計算機管理装置宛てに返

送することを特徴とする。

【００２４】

なお、以上の装置に係る発明は方法に係る発明としても成立し、方法に係る発明は装置に係る発明としても成立する。

また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００２５】

従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱い、といえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【００２６】

本発明によれば、移動計算機が移動先ネットワークに接続し、現在位置の登録メッセージを移動計算機管理装置（ホームエージェント）に送信する際に、移動計算機と移動計算機管理装置との間で、登録された正当なユーザでなければ知得できない情報をやり取りするので、移動計算機を操作しているユーザを認証することができ、より安全に移動計算機を運用することができる。

【００２７】

また、本発明によれば、一旦移動計算機が現在位置登録メッセージを移動計算機管理装置（ホームエージェント）に送信した後も、定期的にユーザ認証を行い、セッション確立後に不正ユーザが移動計算機を使用するケースにも対応できる。また、不正ユーザが一定回数以上認証に失敗した場合に、それ以降の登録を不可とすることができる。

この結果、移動計算機の盗難やユーザ詐称による不正動作を防止できる。

【００２８】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

図１に、本実施形態に係る通信システムの基本構成の一例を示す。

図１の通信システムは、移動ＩＰ（ＲＦＣ２００２）により移動計算機の通信

をサポートしているものとする。なお、移動ＩＰプロトコルでは、移動先ネットワークで移動計算機に対するパケット配送を行うフォーリンエージェントというルータの存在を仮定するモードと、フォーリンエージェントを設けない（移動計算機自身がフォーリンエージェントを兼ねる）Ｃｏ－ｌｏｃａｔｅｄ　Ｃａｒｅ－ｏｆ　ａｄｄｒｅｓｓモードがあるが、本実施形態では、後者を採用するものとして説明する。

【００２９】

図１では、ホームネットワーク１ａ、第１の他部署ネットワーク１ｂ、第２の他部署ネットワーク１ｃがインターネット６を介して相互に接続されており、移動計算機（ＭＮ）２、移動計算機の通信相手（ＣＨ）３は、これらネットワーク内に接続され、または外部ノードとしてインターネット６に接続される。

【００３０】

本実施形態では、ネットワーク１ａの内部をホームポジションとする移動計算機２が他部署ネットワーク１ｂに移動した場合について説明する。

ホームネットワーク１ａには、移動ＩＰプロトコルをサポートするために、移動計算機の移動先の現在位置の情報を管理するホームエージェント（ＨＡ）５が設けられる。管理対象とする移動計算機の台数は任意である。前述したように、移動中の移動計算機２宛に転送されてきたＩＰパケットは、そのホームエージェント５を経由し、移動計算機２の元のアドレス（ホームネットワーク１ａにおけるアドレス）宛のＩＰパケットを移動ＩＰ形式の現在位置アドレス宛てパケット内にカプセル化することで、移動計算機２に対するデータの経路制御を行うことができる。

【００３１】

移動計算機２は、自装置がホームネットワーク外に移動した場合には、移動先のネットワーク（ここでは１ｂ）において、例えばＤＨＣＰやＰＰＰなどのプロトコルにより移動先ネットワークで使用するアドレスを獲得する。アドレスを獲得したら、移動計算機２は、ホームネットワーク１ａのホームエージェント５に現在位置の情報を含む登録メッセージを送信する。

【００３２】

図２に移動計算機２からホームエージェント５に送信される登録メッセージの形式を示す。

フラグ（ＦＬＡＧ）は移動ＩＰの動作モード（カプセル化の方法など）を示す。

【００３３】

Ｌｉｆｅｔｉｍｅはこの登録の有効期限を示す。移動計算機２は有効期限を越えた場合、再度登録メッセージをホームエージェント５に送信し、再登録を行わなくてはいけない。

【００３４】

Ｈｏｍｅ　Ａｄｄｒｅｓｓは移動計算機のホーム位置を、Ｃａｒｅ－ｏｆ　Ａｄｄｒｅｓｓは移動計算機の現在位置を、Ｈｏｍｅ　Ａｇｅｎｔはホームエージェント５のアドレスを示す。

【００３５】

Ｉｄｅｎｔｉｆｉｃａｔｉｏｎは登録に対するＩＤでリプレイ攻撃を防止するために付加される。

Ｅｘｔｅｎｓｉｏｎｓには少なくとも移動計算機２～ホームエージェント５間の（ホスト認証のための）認証情報が含まれる。このＥｘｔｅｎｓｉｏｎ部分を図３に示す。ＳＰＩは両者の間で交換したセキュリティパラメータインデックスを、Ａｕｔｈｅｎｔｉｃａｔｏｒは認証コードを示す。

【００３６】

この登録メッセージをホームエージェント５が受信し、正しく登録処理が行われた場合、図４に示す登録応答メッセージが移動計算機２に返される。ｃｏｄｅには登録成功を示す応答コード０または１が記述される。一方、登録に失敗した場合、図４と同じ形式の登録応答メッセージが移動計算機２に返される。この場合には、種々の登録失敗の理由を示す応答コードが記述される。

【００３７】

以下に、応答コード（Ｒｅｐｌｙ　ｃｏｄｅｓ）の一覧を示す。左側の数字がコードであり、右側の説明がそのコードの示す意味内容である。

＜成功（ｓｕｃｃｅｓｓ）のケース＞

0：登録受諾（registration accepted）

1：登録受諾だが、同時移動バインドはサポートしない（registration accepted, but simultaneous mobility bindings unsupported）

＜フォーリンエージェントのための失敗（failure for Foreign agent）のケース＞

64：理由不明（reason unspecified）

65：管理上の理由で禁止（administratively prohibited）

66：リソースが不十分（insufficient resources）

67：移動ノードの認証失敗（mobile node failed authentication）

68：ホームエージェントが認証に失敗（home agent filed authentidation）

69：要求されたLifeitmeが長すぎる（requested Lifetime too long）

70：要求の形式が正しくない（poorly formed Request）

71：応答の形式が正しくない（poorly formed Reply）

72：要求のカプセル化が使用できない（requested encapsulation unavailable）

73：要求のVan Jacobson圧縮が使用できない（requested Van Jacobson compression unavailable）

80：ホームネットワークが到達不能（ICMPエラー受信）（home network unreachable（ICMP error received））

８１：ホームエージェント・ホストが到達不能（ＩＣＭＰエラー受信）（ｈｏｍｅ　ａｇｅｎｔ　ｈｏｓｔ　ｕｎｒｅａｃｈａｂｌｅ（ＩＣＭＰ　ｅｒｒｏｒ　ｒｅｃｅｉｖｅｄ））

８２：ホームエージェント・ポートが到達不能（ＩＣＭＰエラー受信）（ｈｏｍｅ　ａｇｅｎｔ　ｐｏｒｔ　ｕｎｒｅａｃｈａｂｌｅ（ＩＣＭＰ　ｅｒｒｏｒ　ｒｅｃｅｉｖｅｄ））

８８：ホームエージェントが到達不能（ＩＣＭＰエラー受信）（ｈｏｍｅ　ａｇｅｎｔ　ｕｎｒｅａｃｈａｂｌｅ（ＩＣＭＰ　ｅｒｒｏｒ　ｒｅｃｅｉｖｅｄ））

＜ホームエージェントのための失敗（ｆａｉｌｕｒｅ　ｆｏｒ　Ｈｏｍｅ　ａｇｅｎｔ）のケース＞

１２８：理由不明（ｒｅａｓｏｎ　ｕｎｓｐｅｃｉｆｉｅｄ）

１２９：管理上の理由で禁止（ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ　ｐｒｏｈｉｂｉｔｅｄ）

１３０：リソースが不十分（ｉｎｓｕｆｆｉｃｉｅｎｔ　ｒｅｓｏｕｒｃｅｓ）

１３１：移動ノードの認証失敗（ｍｏｂｉｌｅ　ｎｏｄｅ　ｆｉａｌｅｄ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）

１３２：フォーリンエージェントが認証に失敗（ｆｏｒｅｉｇｎ　ａｇｅｎｔ　ｆａｉｌｅｄ　ａｕｔｈｅｎｔｅｃａｔｉｏｎ）

１３３：登録識別子がマッチしない（ｒｅｇｉｓｔｒａｔｉｏｎ　Ｉｄｅｎｔｆｉｃａｔｉｏｎ　ｍｉｓｍａｔｃｈ）

１３４：要求の形式が正しくない（ｐｏｏｒｌｙ　ｆｏｒｍｅｄ　Ｒｅｑｕｅｓｔ）

１３５：同時移動バインド数が多すぎる（ｔｏｏ　ｍａｎｙ　ｓｉｍｕｌｔａｎｅｏｕｓ　ｍｏｂｉｌｉｔｙ　ｂｉｎｄｉｎｇｓ）

１３６：未知のホームエージェント・アドレス（ｕｎｋｎｏｗｎ　ｈｏｍｅ　ａｇｅｎｔ　ａｄｄｏｒｅｓｓ）

さて、本実施形態では、ホームエージェント５が移動計算機２から登録メッセ

ージを受信しても、すぐには登録処理を行わず、該移動計算機２のユーザ認証を行い、ユーザ認証に成功した場合にのみ登録処理を行う。

【００３８】

以下では、ホームエージェント５が移動計算機２を使用しているユーザを認証するため、チャレンジ～レスポンスによるメッセージを交換する例を、図５を参照しながら説明する。

【００３９】

チャレンジメッセージの形式を図６（ａ）に、レスポンスメッセージの形式を図６（ｂ）に示す。

この例では、移動計算機２が登録要求メッセージをホームエージェント５に送信すると、ホームエージェント５は、まず、認証情報を調べホスト認証を行う。そして、ホスト認証に成功しならば、ホームエージェント５は、パスワード入力を要求するチャレンジメッセージを、移動計算機２に返信する。

【００４０】

移動計算機２は、このチャレンジメッセージを受けると、メッセージを表示するなどして、ユーザにパスワード入力を促す。そして、パスワードが入力されたならば、このユーザが入力したパスワードを書き込んだレスポンスメッセージを、ホームエージェント５に送信する。

【００４１】

レスポンスメッセージを受け取ったホームエージェント５は、予めホームネットワーク駐在時に該移動計算機に対応して登録してあったパスワードと比較を行い、照合の結果、該移動計算機から返されたパスワードが正しいものであることが確認されたならば、現在位置の登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置を登録して移動計算機２へのデータパケットの転送を開始する。

【００４２】

なお、以降の再登録メッセージについては、同様の手順でその都度ユーザ認証を行う方法、何回かに一度だけユーザ認証を行う方法、ユーザ認証を行わない方法など種々の方法が考えられる。

【0043】

また、上記では、移動計算機からホームエージェント5にパスワードを返したが、パスワードとユーザIDの組を返し、ホームエージェント5はこの組が予め登録されたものかどうか調べることによりユーザの正当性を判断するようにしてもよい。

【0044】

上記の例では、単純なパスワード照合によるユーザ認証の例を示したが、ユーザ認証には他の方法を使用することもできる。例えばワンタイムパスワードにより認証を行う方法が考えられる。以下ではワンタイムパスワードを用いたユーザ認証の例を図7を参照しながら説明する。

【0045】

チャレンジメッセージの形式を図8（a）に、レスポンスメッセージの形式を図8（b）に示す。

この例では、移動計算機2が登録要求メッセージをホームエージェント5に送信すると、まず、ホームエージェント5は認証情報を調べホスト認証を行っう。そして、ホスト認証に成功したならば、この移動計算機2を使用するユーザの登録情報をもとにしてワンタイムパスワードのチャレンジコードを求める。そして、このチャレンジコードを付加した、パスワード入力を要求するチャレンジメッセージを、移動計算機2に返信する。

【0046】

チャレンジメッセージを受信した移動計算機2は、別のユーティリティを使用して、このチャレンジメッセージ内のワンタイムパスワードチャレンジコードとユーザから入力されたパスワードとが反映された、このチャレンジに対して応答するデータを算出し、このデータを含むレスポンスメッセージをホームエージェント5に送信する。

【0047】

レスポンスメッセージを受け取ったホームエージェント5は、登録情報をもとに移動計算機2で行われたものと同じ計算を行って、データの照合を行い、正しければ、現在位置の登録を許可するものとし、登録成功の応答コードを含む登録

応答メッセージを返信するとともに、現在位置を登録して移動計算機２へのデータパケットの転送を開始する。

【００４８】

なお、以降の再登録メッセージについては、同様の手順でその都度ユーザ認証を行う方法、何回かに一度だけユーザ認証を行う方法、ユーザ認証を行わない方法など種々の方法が考えられる。

【００４９】

なお、上記の各例においてユーザ認証が失敗に終わった場合、ただちにユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよい。あるいは、チャレンジメッセージとレスポンスメッセージのやり取りを規定回数繰り返してもユーザ認証に成功しなかった場合に、ユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよい。

【００５０】

上記の２つの例では、移動計算機２が移動先ネットワークに接続し、登録処理を開始する時点でのユーザ認証について示したが、実際の運用では登録完了後に不正ユーザが移動計算機２を不正使用して（例えば、正規ユーザが移動計算機２を繋いだまま離席し、その間に不正ユーザが使用するなど）、ホームネットワーク内の情報を漏洩させるようなケースにも対応することが望ましい。

【００５１】

このための対応処理として、移動計算機２が一旦登録処理に成功した後も、一定時間毎にホームエージェント５から移動計算機２にユーザ認証要求メッセージを送信することが考えられる。そのような例を図９および図１０を参照しながら説明する。図９はこの場合にホームエージェント５に付加する機能を示すブロック図の一例であり、図１０はその手順の一例である。

【００５２】

図９の機能を持つホームエージェント５において、予めユーザ（管理者等）が指定する再ユーザ認証インターバル時間をレジスタ５１に入力する。

ある移動計算機２について、ユーザ認証シーケンスを実行すると（ステップＳ

１５）、その移動計算機２に対応するタイマカウンタ５２は０にクリアされる（ステップＳ１１）。なお、最初のユーザ認証シーケンスは、例えば図５や図７のように、ある移動計算機について、移動後の最初の登録メッセージを受信したときである。

【００５３】

その後、移動計算機から現在位置の再登録メッセージを受信し、再登録を行う毎に、該当するタイマカウンタ５２が経過時間に更新される（ステップＳ１２～Ｓ１４）。

【００５４】

この位置再登録時には、レジスタ５１のインターバル時間と該当するタイマカウンタ５２の値が比較部５３にて比較され（ステップＳ１４）、タイマカウンタ５２の内容がインターバル時間より小さい場合は、ユーザ認証なしに現在位置の再登録および登録成功メッセージの送信を行う。

【００５５】

一方、タイマカウンタ５２の内容がインターバル時間に達した場合には、例えば図５や図７のようなユーザ認証シーケンスを、再度実行する（ステップＳ１５）。ユーザ認証が正しく行われると、現在位置の再登録を許可するものとし、登録成功の応答コードを含む登録応答メッセージを返信するとともに、現在位置の再登録を行って移動計算機２へのデータパケットの転送を継続し、また、再度、該当するタイマカウンタ５２は０にクリアされる（ステップＳ１１）。

【００５６】

そして、ユーザ認証なしの位置再登録およびタイマーカウンタの更新の繰り返えしと、一定時間経過した場合のユーザ認証とこれに成功した際の位置再登録といった、一連の手順が、現在位置の有効期限の経過またはユーザ認証の失敗または位置登録の失敗まで繰り返される。

【００５７】

また、ユーザ認証が失敗に終わった場合、前述したように、ただちにユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよいし、チャレンジメッセージとレスポンスメッセージのやり取りを規定回

数繰り返してもユーザ認証に成功しなかった場合に、ユーザ認証不成功を示すコードを含む登録応答メッセージを該移動計算機に返すようにしてもよい。

【００５８】

なお、上記では、一定時間経過ごとにユーザ認証を行う例を示したが、再登録メッセージを受信するごとにユーザ認証を行う方法、何回かに一度だけユーザ認証を行う方法など、種々の方法が考えられる。

【００５９】

ところで、例えば移動計算機２が盗難されて、不正ユーザがホームネット外部から登録要求を行おうとする場合、図５、図７、図１０で例示したようなユーザ認証を用いれば、（通常の方法ではユーザ認証を成功させるのは極めて困難であるので）現在位置の登録ができず、不正使用はできない。しかし、不正ユーザがパスワードを総当たりで破ろうとするなどして、登録（ユーザ認証）メッセージの送受信を繰り返し行うことで、ホームネットワークのトラフィックが混雑し、正常な運用ができなくなるおそれがある。また、不正ユーザから辞書などを使ったパスワードの類推攻撃を受ける可能性も考えられる。

【００６０】

これらの問題に対応するため、一定回数以上のユーザ認証レスポンス失敗を繰り返した場合、以降の移動計算機２からのメッセージ送出を不可能とすることが考えられる。そのような例を図１１および図１２を参照しながら説明する。図１１はこの場合に移動計算機２に付加する機能を示すブロック図の一例であり、図１２はその手順の一例である。

【００６１】

図１１の機能を持つ移動計算機２において、予めユーザ（システム管理者あるいは移動計算機の使用者等）が指定する連続ユーザ認証失敗回数をレジスタ１２１に入力する（ステップＳ２１）。

【００６２】

移動計算機２がユーザ認証に失敗した旨のメッセージをホームエージェント５から受信する毎に、（予め初期化しておいた）認証失敗回数カウンタ１２２をインクリメントする（ステップＳ２２～Ｓ２５）。一方、ユーザ認証に成功したら

（ステップＳ２３でＹｅｓの場合）、認証失敗回数カウンタ１２２は０にリセットされる。

【００６３】

しかして、ステップＳ２５において、比較部１２３にてレジスタ１２１と認証失敗回数カウンタ１２２の値を比較して、それらが一致したら（ステップＳ２５でＹｅｓの場合）、移動計算機２はメッセージ送出停止制御部１２４を起動し、これ以降の一切のメッセージ送出を停止する（ステップＳ２６）。メッセージ送出停止制御部１２４によるメッセージ送信抑止を解除するには、この移動計算機２に固有のホームエージェント内に格納されている情報を使用しなくてはいけないものとする。

【００６４】

上記では移動計算機にメッセージ送信抑止機能を設けたが、他の例（図１３、図１４）として、ホームエージェント５側でユーザ認証失敗回数カウンタ９２を持ち、失敗回数レジスタ９１の値がこれに同じくなったら、それ以降いかなるメッセージが送信されても登録を成功させないという方法も考えられる。

【００６５】

この場合、図１３の機能を持つホームエージェント５において、予めユーザ（システム管理者等）が指定する連続ユーザ認証失敗回数を、各移動移動計算機に対応するレジスタ１５１に入力する（ステップＳ３１）。

【００６６】

ホームエージェント５では、ユーザ認証が成功しなかった毎に、該当する（予め初期化しておいた）認証失敗回数カウンタ１５２をインクリメントする（ステップＳ２３～Ｓ２５）。一方、ユーザ認証に成功したら（ステップＳ３３でＹｅｓの場合）、認証失敗回数カウンタ１５２は０にリセットされる。

【００６７】

しかして、ステップＳ３５において、比較部１５３にてレジスタ１５１と認証失敗回数カウンタ１５２の値を比較して、それらが一致したら（ステップＳ３５でＹｅｓの場合）、ホームエージェント５は登録メッセージ受付拒否制御部１５４を起動し、これ以降の当該移動計算機２からの一切の登録メッセージの受付を

拒否する（ステップＳ２６）。

【００６８】

なお、この方法は、不要なメッセージのやり取りを防止できない点で、図１１、図１２の例よりセキュリティ的な基準は多少甘いとも考えられるが、例えばサイトのポリシーなどに依って図１１と図１３のいずれの方法を使用するかを選択するなどすればよい。

【００６９】

また、上記した２つの例の他に、規定回数の失敗は移動計算機２側で検出し、これを移動計算機２からホームエージェント５に通知し、ホームエージェント５はそれ以降の当該移動計算機２からの一切の登録メッセージの受付を拒否するようにする方法も考えられる。

【００７０】

上記の３つの例において、規定回数の認証の失敗を検出した時点で当該移動計算機２の登録を削除してもよいし、有効期限までは転送をサポートするようにしてもよい。

【００７１】

さて、従来の移動ＩＰ方式におけるセキュリティ対策では、ホスト単位の成り済ましには対応されているが、不正ユーザが正規ユーザに成り済ますという攻撃には極めて弱い、といえる。そのため、移動先（外部ネットワーク）に内部ネットワークの機密情報が取り出されてしまうおそれがあった。

【００７２】

本実施形態によれば、移動計算機が移動先ネットワークに接続し、現在位置の登録メッセージをホームエージェントに送信する際に、移動計算機とホームエージェントとの間で、登録された正当なユーザでなければ知得できない情報をやり取りするので、移動計算機を操作しているユーザを認証することができ、より安全に移動計算機を運用することができる。

【００７３】

また、本実施形態によれば、一旦移動計算機が現在位置登録メッセージをホームエージェントに送信した後も、定期的にユーザ認証を行い、セッション確立後

に不正ユーザが移動計算機を使用するケースにも対応できる。また、不正ユーザが一定回数以上認証に失敗した場合に、それ以降の登録メッセージ送出あるいは登録メッセージの受け付けを不許可とすることができる。

【００７４】

この結果、移動計算機の盗難やユーザ詐称による不正動作を防止できる。

なお、本実施形態では、Ｃｏ－ｌｃａｔｅｄ　Ｃａｒｅ－ｏｆ　Ａｄｄｒｅｓｓモードによる通信システムについて説明したが、本発明は、フォーリンエージェントの存在を仮定した移動通信システムにも適用可能である。

【００７５】

また、本発明は、ＲＦＣ２００２に示される移動ＩＰだけでなく、他の様々な移動通信プロトコルに対しても適用可能である。

また、以上の各機能、例えば処理の部分の他、移動計算機がユーザ認証を行う再登録回数を指定する設定カウンタ、登録回数をカウントするカウンタなどはハードウェアとしてもソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００７６】

【発明の効果】

本発明によれば、移動先ネットワークに接続した移動計算機から現在位置の登録メッセージが移動計算機管理装置に送信された際に、移動計算機と移動計算機管理装置との間で、登録された正当なユーザでなければ知得できない情報をやり取りするので、移動計算機を操作しているユーザを認証することができる。

この結果、移動計算機の盗難やユーザ詐称による不正動作を防止することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係るネットワークの基本構成を示す図

【図２】

同実施形態に係る移動計算機の送信する登録要求メッセージ形式を示す図

【図３】

同実施形態に係る移動計算機の送信するホスト認証のための拡張した登録要求メッセージを示す図

【図４】

同実施形態に係るホームエージェントからの登録要求応答メッセージを示す図

【図５】

同実施形態に係るユーザ認証方式を説明するための図

【図６】

ユーザ認証のためのメッセージの形式の一例を示す図

【図７】

同実施形態に係る他のユーザ認証方式を説明するための図

【図８】

ユーザ認証のためのメッセージの形式の他の例を示す図

【図９】

位置再登録に伴うユーザ認証を行うホームルータの構成を示す図

【図１０】

図９のホームルータの動作手順を示すフローチャート

【図１１】

ユーザ認証に関する攻撃に対処する移動計算機の構成を示す図

【図１２】

図１１の移動計算機の動作手順を示すフローチャート

【図１３】

ユーザ認証に関する攻撃に対処するホームルータの構成を示す図

【図１４】

図１１のホームエージェントの動作手順を示すフローチャート

【符号の説明】

１ａ，１ｂ，１ｃ…ネットワーク

2…移動計算機

3…通信相手計算機

5…ホームエージェント

6…インターネット

51…インターバルレジスタ

52…タイマーカウンタ

53…比較部

121…失敗回数レジスタ

122…失敗回数カウンタ

123…比較部

124…メッセージ送出停止制御部

151…失敗回数レジスタ

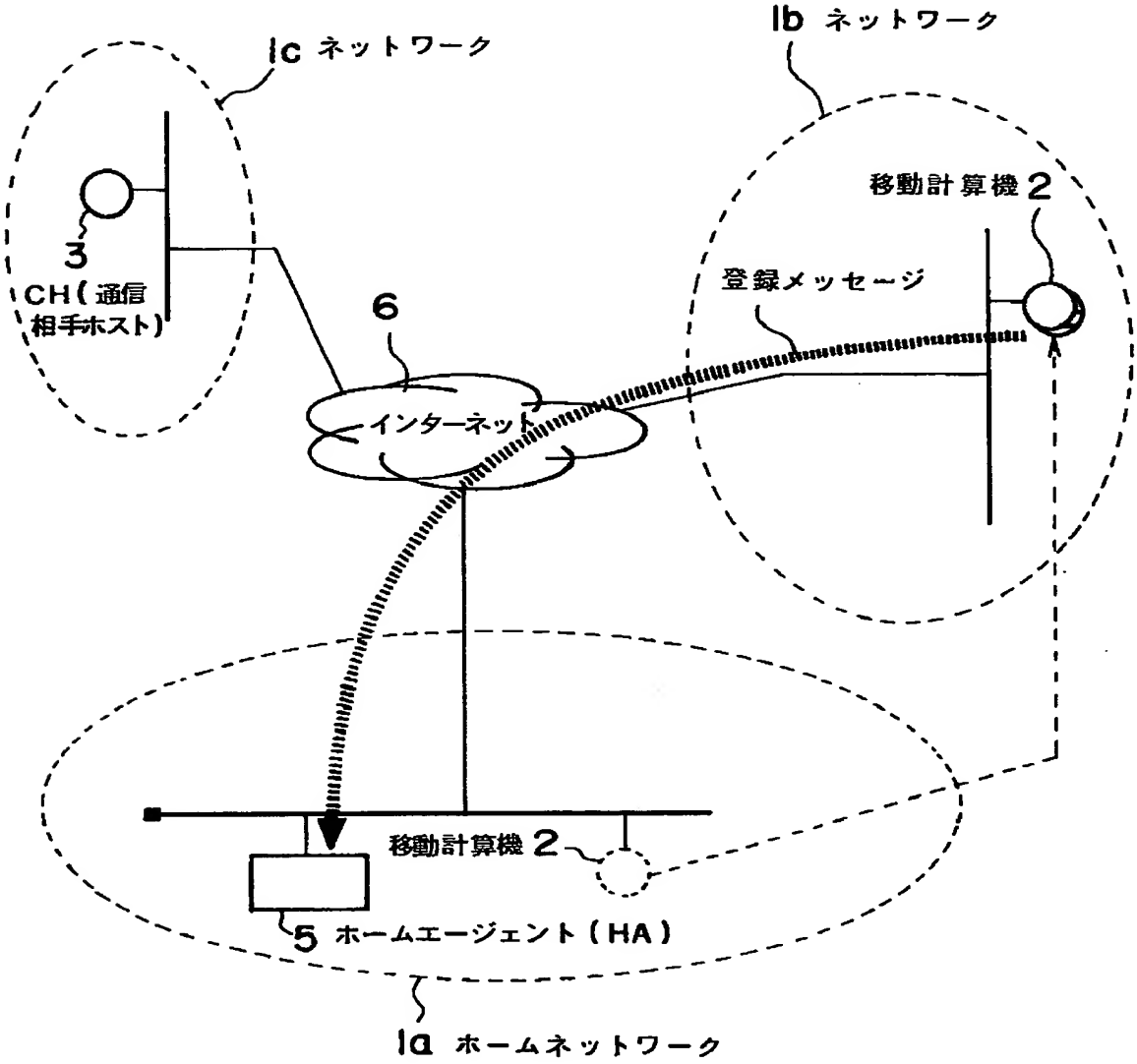
152…失敗回数カウンタ

153…比較部

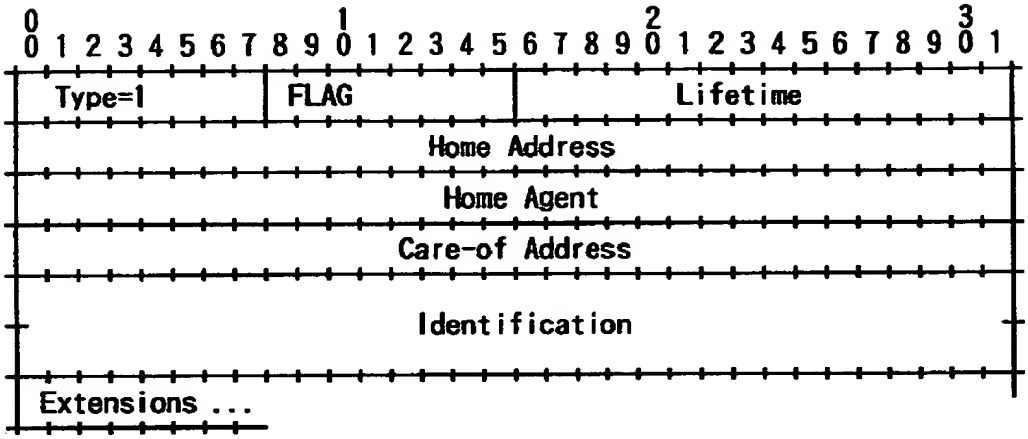
154…登録メッセージ受付拒否制御部

【書類名】　　図面

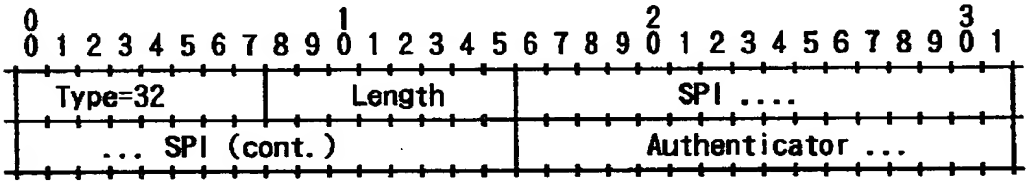
【図１】


1c ネットワーク
1b ネットワーク
移動計算機 2
3
CH（通信
相手ホスト）
登録メッセージ
6
インターネット
移動計算機 2
5 ホームエージェント（HA）
1a ホームネットワーク

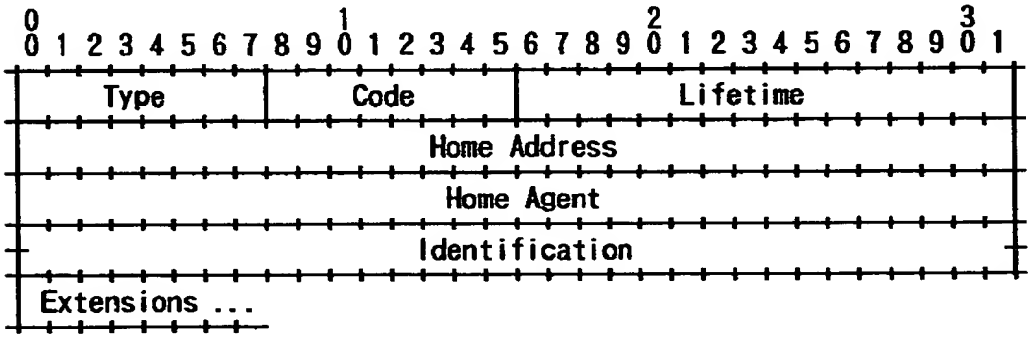
【図２】


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type=1
FLAG
Lifetime
Home Address
Home Agent
Care-of Address
Identification
Extensions ...

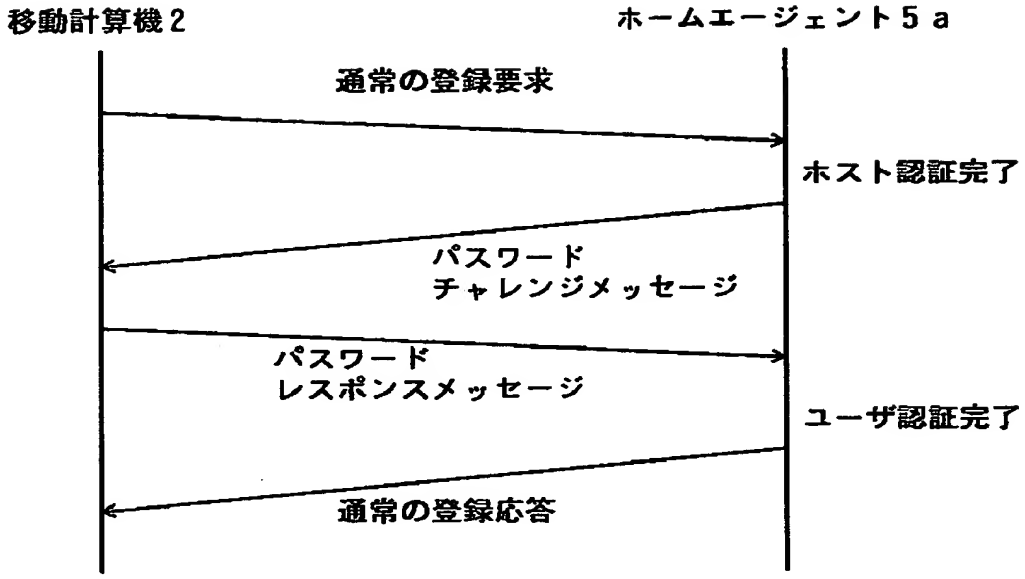
【図３】


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type=32
Length
SPI ....
... SPI (cont.)
Authenticator ...

【図４】


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Code
Lifetime
Home Address
Home Agent
Identification
Extensions ...

【図５】



【図６】

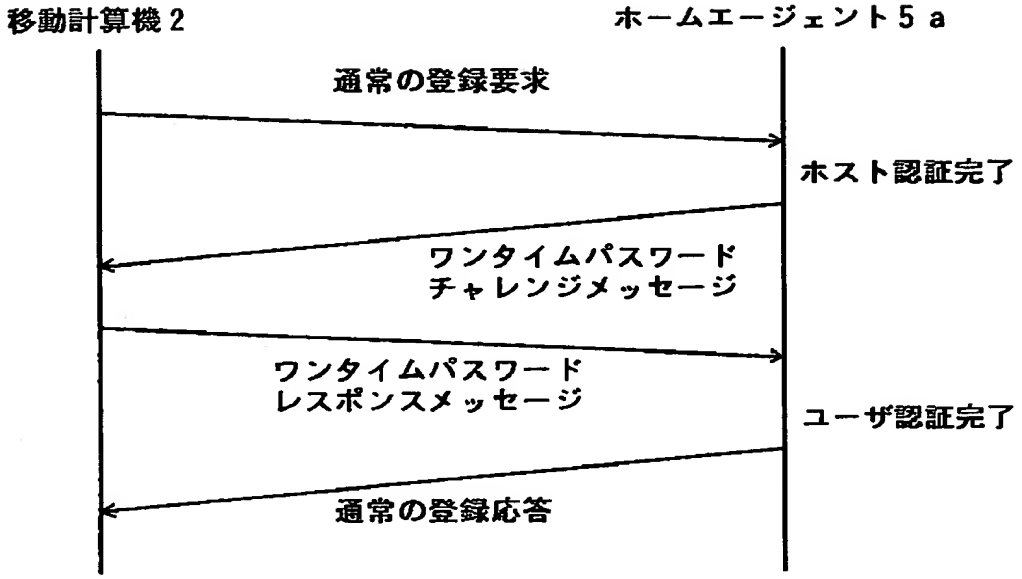
Type=137(passwd challenge)
Home address
Home agent
Identification

(a)

Type=138(passwd response)
Home address
Home agent
Identification
Password string (variable length)

(b)

【図7】



【図8】

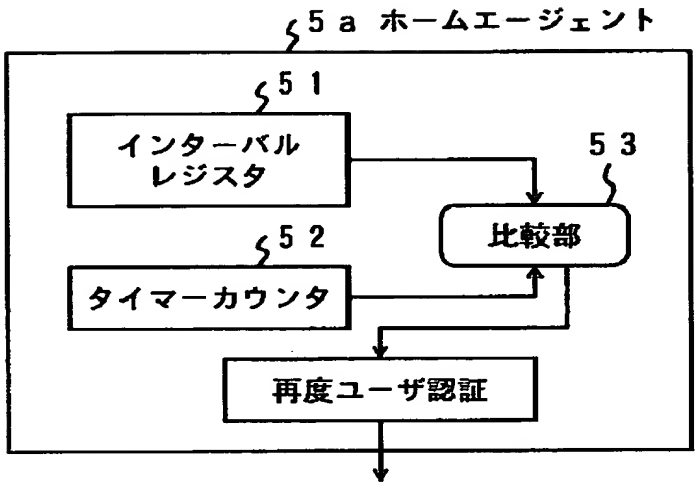
Type=139(onetime passwd challenge)
Home address
Home agent
Identification
challenge code

(a)

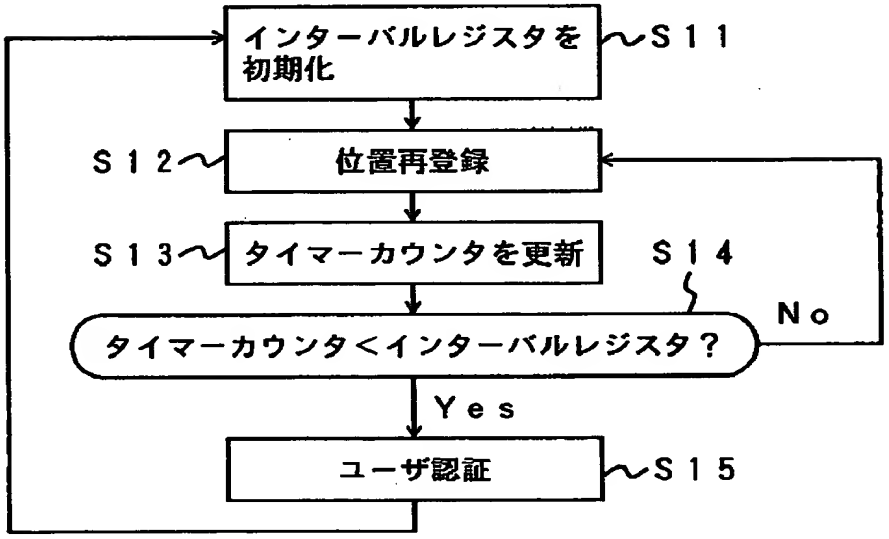
Type=140(onetime passwd response)
Home address
Home agent
Identification
Password string (variable length)

(b)

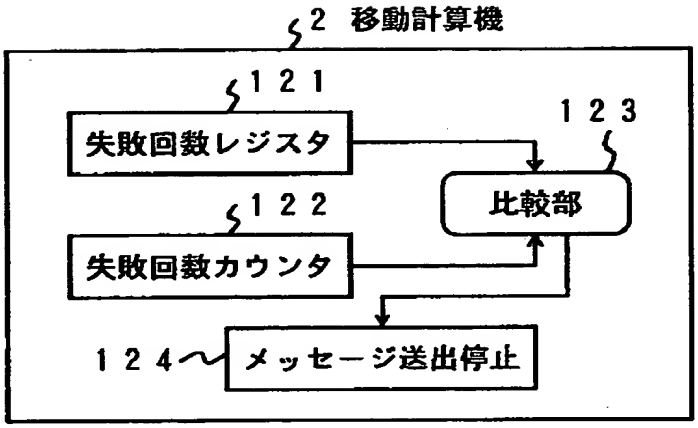
【図9】


5a ホームエージェント
51
インターバル
レジスタ
53
比較部
52
タイマーカウンタ
再度ユーザ認証

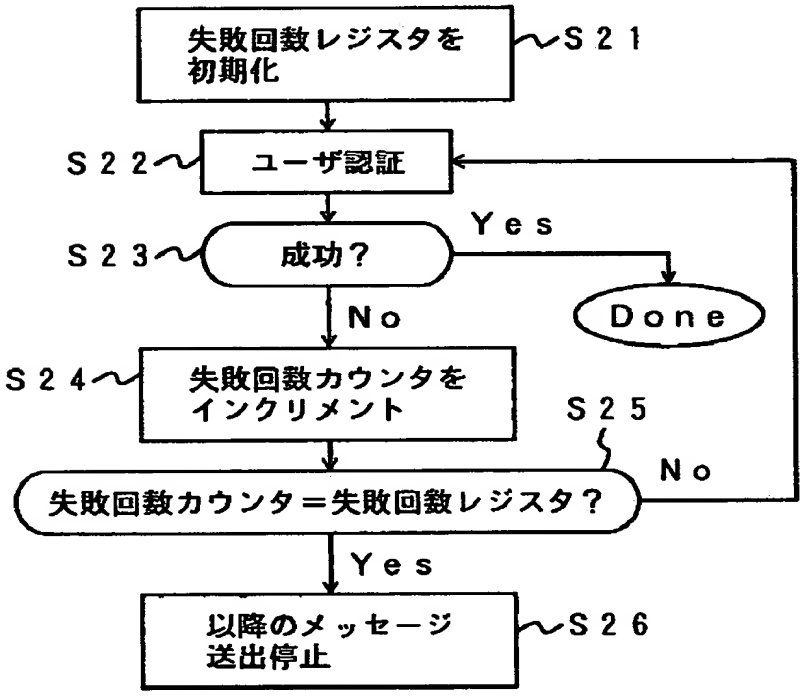
【図10】


インターバルレジスタを
初期化
S11
S12
位置再登録
S13
タイマーカウンタを更新
S14
No
タイマーカウンタ＜インターバルレジスタ？
Yes
ユーザ認証
S15

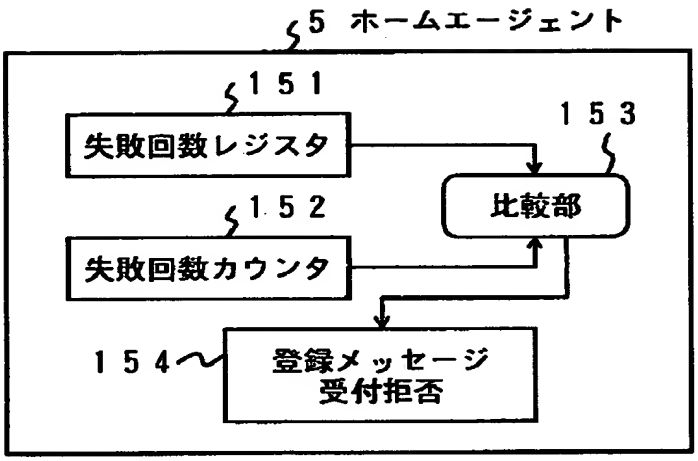
【図１１】


2　移動計算機
121
失敗回数レジスタ
123
比較部
122
失敗回数カウンタ
124
メッセージ送出停止

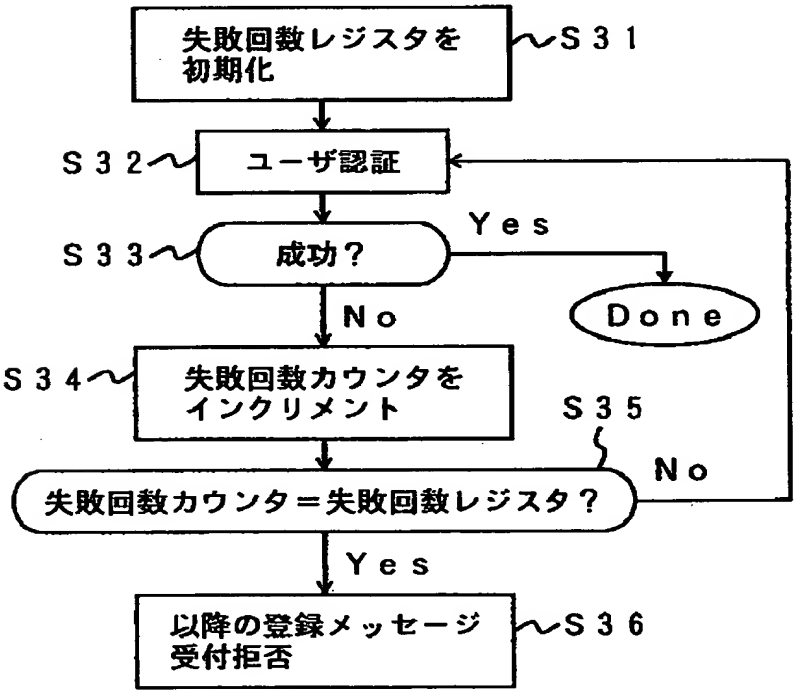
【図１２】


失敗回数レジスタを
初期化
S21
S22
ユーザ認証
S23
成功？
Yes
Done
No
S24
失敗回数カウンタを
インクリメント
S25
No
失敗回数カウンタ＝失敗回数レジスタ？
Yes
以降のメッセージ
送出停止
S26

【図１３】


5 ホームエージェント
151
失敗回数レジスタ
153
比較部
152
失敗回数カウンタ
154
登録メッセージ
受付拒否

【図１４】


失敗回数レジスタを
初期化
S31
S32
ユーザ認証
S33
成功？
Yes
Done
No
S34
失敗回数カウンタを
インクリメント
S35
No
失敗回数カウンタ＝失敗回数レジスタ？
Yes
以降の登録メッセージ
受付拒否
S36

【書類名】　　要約書

【要約】

【課題】　移動計算機が移動先ネットワークから現在位置の登録メッセージを移動計算機管理装置に送信する際に、移動計算機を操作しているユーザを認証することのできる移動計算機管理装置を提供すること。

【解決手段】　ネットワーク間を移動して通信を行うことが可能な移動計算機の移動位置情報を管理し移動計算機宛のパケットをその現在位置に転送する移動計算機管理装置であって、移動計算機から発信された現在位置の情報を含む新規の登録メッセージを受信した場合、移動計算機に対してユーザ認証のための情報の返送を要求するメッセージを送信し、このメッセージを送信した移動計算機からユーザ認証のための情報として移動計算機へのユーザ入力に基づく情報が書き込まれたメッセージが返送されてきた場合、ユーザ入力に基づく情報を判定してユーザの正当性が確認されたならば、移動計算機の現在位置の登録を許可する。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
　【識別番号】　000003078
　【住所又は居所】　神奈川県川崎市幸区堀川町７２番地
　【氏名又は名称】　株式会社東芝
【代理人】　申請人
　【識別番号】　100058479
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　鈴江　武彦
【選任した代理人】
　【識別番号】　100084618
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　村松　貞男
【選任した代理人】
　【識別番号】　100068814
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　坪井　淳
【選任した代理人】
　【識別番号】　100092196
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　橋本　良郎
【選任した代理人】
　【識別番号】　100091351
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　河野　哲
【選任した代理人】
　【識別番号】　100088683
　【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
　【氏名又は名称】　中村　誠
【選任した代理人】

【識別番号】　100070437
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許事務所内
【氏名又は名称】　河井　将次

出　願　人　履　歴　情　報

識別番号　　〔000003078〕

1．変更年月日　　1990年　8月22日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町72番地
氏　名　株式会社東芝